



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,984	01/16/2004	Harry Snyder	2003P00652 US01	7911
7590 08/06/2008				
Alexander J. Burke Intellectual Property Department 5th Floor 170 Wood Avenue South Iselin, NJ 08830			EXAMINER VY, HUNG T	
			ART UNIT 2163	PAPER NUMBER
			MAIL DATE 08/06/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/758,984
Filing Date: January 16, 2004
Appellant(s): SNYDER ET AL.

Alexander J. Burke
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 05/27/2008 appealing from the Office action mailed 12/27/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0061279	Liewellyn et al.	03-2003
2003/0061279	Gavrila et al.	02-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraph of 35 U.S.C. § 102 in view of the AIPA and H.R. 2215 that forms the basis for the rejections under this section made in the attached Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 7, and 10-19 are rejected under 35 U. S. C. § 102 (e) as being anticipated by Llewellyn et al. (U.S. pub. No. 2003/0061279 A1).

Regarding to claim 1, Llewellyn et al. discloses a system enabling individual organizations of a plurality of different organizations (i.e., “many enterprises (companies, organizations, foundations, and the like) may rely on a central server to provide access to the Internet for all users on a local area network or wide area network served by the enterprise server owned by that company” (0009)) to manage access of their own respective employees (i.e., “The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization”) (0109)) to at least one remotely located application (i.e., “an application 86” (0078)) hosted by an application service provider (i.e., The server farm 99 may be an Application Service Provider (“ASP”) farm 99. An ASP typically deploys, host, and manger access to an application”) (0078)), comprising:

at an application service provider (i.e., *"The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application"*) (0078)) **site**,

at least one database (i.e., *"The application profiles 188 may be embodied as a memory mapped files rather than files stored on a storage device 16 such as a hard drive 16"* (0132) and Examiner asserts that in the specification defines *"the database 138, otherwise called a memory device"* (0042), and Llewellyn et al.

discloses application 479, application profiles and image (user interface) are stored in memory 14 (fig. 8, 14))

asset containing data representing a plurality of user interface images (i.e., *"A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and horizontal scaleability"* (0077) or *"many applications 86 make use of API calls which draw simple shapes to display, often, an application 86 will make many such API calls to render an image"* (0089))

associated with a corresponding plurality of organizations (Fig. 15 shows that image "Subscriber entry Point 500" associated with "client Module 80a" and "provider Entry Point 502" associated with "Client Module 80b" and *"The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization"*) (0109) and (Figs. 14-15)), and a plurality of executable procedures associated with the

corresponding plurality of user interface images (i.e., *"A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and horizontal scaleability"* (0077)), an executable procedure supporting a user of a particular

organization of said plurality of organization (i.e., *"companies, organizations"* (0009)) in

managing access of employees of the particular organization (i.e., *"The authorization module 198 may also query a central services module 240 or some other database in order to discover which applications a particular user or workstation 94 is allowed to access"* (0109) and *"allowing user to access data and functionality specific to their session with an application 86"* (0092) or *"An entry point 480a,b may have a user interface 482a,b through which a user may control the application and view output. Each user interface 482a,b*

may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176)) to an application ("allowing user to access data and functionality specific to their session with an application 86" (0092))) hosted by an application service provider (i.e., "The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application" (0078), and used by said plurality of organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)); and

a command processor (i.e., "processor 12 for processing software commands" (0069) (Fig. 1)) employing the at least one database (i.e., "a data entry application on a workstation that accesses a database that is on a server" (0013)) for initiating execution of a particular executable procedure organization (i.e., "companies, organizations" (0009)) in response to a command initiated at a remote location associated with the particular organization (Fig. 15 shows that image "Subscriber entry Point 500" associated with "Workstation 94a" and "provider Entry Point 502" associated with "Workstation 94b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109) and "In entry point 480a,b may have a session initiation module 488a,b that allows users to connect to an application 479" (0177)) using a particular user interface image (i.e., "a subscriber entry point 500 may include a display module 510 which may capture screen shots of a subscriber's workstation 94a" (0181 and fig. 15)) associated with the particular executable procedure and with the particular organization (i.e., "configuration data associated with a particular user or organization" (109)), the particular executable procedure supporting the user in managing and granting access of an employee (i.e., "An ASP typically deploys, hosts, and manages access to an application, such

Art Unit: 2162

as an application 86, to multiple users from a **centrally managed facility**" 0078)) of the particular organization to an application, an authorization processor for authorizing access of the user to a particular user interface image (i.e., "display module 510 which may capture **screen shots of a subscriber's workstation 94a**" (0181) or "enable one remote user to see and control the **screen** of a second remote user")(0027) or "The authorization module 198 may perform other functions in order to control access to services provided by the server module 160" (0109)) without intervention by the application service provider (Based on specification defines "without intervention by the application service" as *managing their accounts, without requiring intervention by or cooperation with another party*" (0010) and Llewellyn et al. discloses "the entry point **management module 148** may allow a user to connect to a particular entry point of an application 86,...allowing user to access data and **functionality specific to their session with an application**"(0092) and Examiner asserts that the client can access to particular entry point and **management their functionality and data** without intervention with another the client. For particular, example, Fig. 15 shows client 80a can access to 500 to manage their functionality and data without intervention by client 80b) and excluding access by employees of organizations other than said particular organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" (0109) and "The authorization module 198 may also query a central services module 240 or some other database in order to discover which **applications a particular user or workstation 94 is allowed to access**" (0109) and "**allowing user to access data and functionality specific to their session with an application 86**" (0092) or "An entry point 480a,b may have a user interface 482a,b through which a user may control the application and **view output**. Each user interface 482a,b **may be different and allow access to data 484a,b and methods 484a,b** unique to a particular entry point 480a,b. For example entry point 480a may have a **user interface 482a that allows a user to access data 484a and methods 486a**. Data 484a and methods 486a may be available **exclusively to users accessing the application through entry point 480a**" (0176).

Regarding claim 2, Llewellyn et al. discloses wherein said at least one database (i.e., "a data entry application on a workstation that accesses a **database** that is on a server" (0013)), said command processor (i.e., "processor 12 for processing software commands" (0069) (Fig. 1)) , said application and associated application data specific to said particular organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)), are located at said application service provider (i.e., The **server farm 99** may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application") (0078)) site behind a firewall (i.e., "communicate through HTTP handshaking. This may **help past fire walls** and work with fire walls and server farms" (0203)) and accessed through said firewall by users of said plurality of organization (i.e., "The server may be accessed by a one click connection. Such an icon may be on the desktop of a user's workstation 78, 90, 94" (0203)) and include an authorization processor for authorizing access of the user to the particular user interface image (i.e., "A **server farm 99** may be thought of as a group of servers that are linked together as a single system **image** to provide centralized administration and horizontal scalability" (0077)) and the associated particular executable procedure in response to received identification information (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)).

Regarding claim 3, Llewellyn et al. discloses wherein said particular executable procedure and said particular user interface (i.e., "image display module 510 which may capture screen shots of a subscriber's workstation 94a" (0181)) are specifically associated with said particular organization "An entry point 480a, b may have a **user interface 482a, b** through which a user may control the application and view output. **Each user interface 482a, b** may be different and allow access to data

Art Unit: 2162

484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176)) and

the authorization processor excludes access of the user and employees of the particular organization (i.e., *"The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)) to user interface images (i.e., "A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and horizontal scalability" (0077)), and executable procedures and data associated with organizations other than the particular organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109))*

Regarding claim 7, Llewellyn et al. discloses wherein the plurality of executable procedures comprises a plurality of sets of executable procedures associated with the corresponding plurality of user interface images organization (i.e., *"many applications 86 make use of API calls which draw simple shapes to display, often, an application 86 will make many such API calls to render an image" (0089) or "the methods 486a of a subscriber entry point 500 may include a display module 510 which may capture screen shots of a subscriber's workstation 94a. The provider entry point 502 may have a viewing module 512 that displays the captured display the screen shots on the provider's workstation 94b. In this manner the provider may see whatever the subscriber is seeing on his/her computer screen" (0181) and Examiner asserts plurality of user interface ("the entry point 500", "entry point 502") can be viewed and associated with particular origination (workstation 94a, 94b)) and the command processor employs (i.e., "processor 12 for processing software commands" (0069) (Fig. 1)) the at least one database (i.e., "a data entry application on a workstation that accesses a database that is on a server" (0013)) for initiating execution of a*

Art Unit: 2162

particular executable procedure in a particular set of executable procedures in response to a command initiated using the particular executable procedure in a particular set of executable procedures (*i.e.*, “the second memory storing a client module executable by the second processor” (claim 4)) in response to a command initiated using the particular user interface image (*i.e.*, “The **client module 80a** may then **initiate 562 a session** with the subscriber application 479” (0187) and Examiner asserts plurality of user interface (“the entry point 500”, “entry point 502”) can be viewed and associated with particular origination (workstation 94a, 94b)).

Regarding claim 10, Llewellyn et al. discloses wherein an executable procedure enables the user to amend information used in authorizing a particular employee of an organization to access (*i.e.*, “an editing module 256 **may permit editing** by an appropriate authorized individual accessing the data records 250”) (0118)) the application hosted by the application service provider (*i.e.*, “The **server farm 99** may be an Application Service Provider (“ASP”) farm 99. An ASP typically deploys, host, and manger access to an application” (0078)).

Regarding claim 11, Llewellyn et al. discloses wherein an authorization processor for authorizing access of the employee of the particular organization to the particular user interface image (*i.e.*, “**many applications 86** make use of API calls which draw simple shapes to display, often, an application 86 will make many such API calls to render an image” (0089) or “the methods 486a of a subscriber entry point 500 may include a display module 510 which may capture screen shots of a subscriber’s workstation 94a. The provider entry point 502 may have a **viewing module 512 that displays the captured display the screen shots on the provider’s workstation 94b**. In this manner the provider may see whatever the subscriber is seeing on his/her computer screen” (0181) and Examiner asserts plurality of user interface (“the entry point 500”, “entry point 502”) can be viewed and associated with particular origination (workstation 94a, 94b)) and the associated particular executable procedure in response to received

employees identification information (i.e., “The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization”) (0109) and “**identification data 268**, associations 270, and **authorizations 272**” (0123)) .

Regarding claim 12, Llewellyn et al. discloses wherein the authorization processor uses a combination of an organization specific identifier and received employee identification information (i.e., “**identification data 268**, associations 270, and **authorizations 272**” (0123)) in providing an employee access to the application hosted by the application service provider (i.e., *The server farm 99 may be an Application Service Provider (“ASP”) farm 99. An ASP typically deploys, host, and manger access to an application”) (0078)*) to prevent replication of user identification information between two employees of different organization of the plurality of organizations (i.e., “identification data 268 may include data **identifying a user or identifying others associated** with a user...authorization data 272 may include data indicating things that **a user is authorized to do or places that a user is authorized to access**” (0124) and “The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization”) (0109) and Examiner asserts that the system “configuration data associated with a particular user or organization” and “prevent unauthorized access to a server” (0110), therefore, the system will “prevent replication of user identification information”)

Regarding claim 13, Llewellyn et al. discloses wherein **at least one** of machine code (i.e., “rewriting of computer code to customize software application” (0026)), a compiled computer language (i.e., “running on a remote computer are expressly written and compiled to make API calls to an X client on the server” (0024)).

Regarding claim 14, Llewellyn et al. discloses wherein the particular executable procedure comprises a template procedure customized by at least one of the user and a technician (i.e., “central store of configuration information, profiles, **templates**, certification information, associations, authorizations, and the like” (0072) or “templates 264 may include pre-configured data or data structures useful in providing services to users of the invention” (0123)).

Regarding claim 15, Llewellyn et al. discloses wherein at least one of, the command is initiated at a user site via a particular user interface image communicated to the user site (i.e., “many applications 86 make use of API calls which draw simple **shapes** to display, often, an application 86 will make many such API calls to render an image” (0089) or “the methods 486a of a subscriber entry point 500 may include a display module 510 which may capture screen shots of a subscriber’s workstation 94a. The provider entry point 502 may have a **viewing module 512 that displays the captured display the screen shots on the provider’s workstation 94b**. In this manner the provider may see whatever the subscriber is seeing on his/her computer screen” (0181) and Examiner asserts plurality of user interface (“the entry point 500”, “entry point 502”) can be viewed and associated with particular origination (workstation 94a, 94b)).

Regarding to claim 16, Llewellyn et al. discloses a system enabling individual organizations of a plurality of different organizations (i.e., “many enterprises (companies, organizations, foundations, and the like) may rely on a central server to provide access to the Internet for all users on a local area network or wide area network served by the enterprise server owned by that company” (0009)) to manage access of their own respective employees (i.e., “The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization”) (0109)) to at least one remotely located application (i.e., “an application 86”) (0078)) hosted by an application service provider (i.e., The server farm 99 may be an Application Service Provider (“ASP”) farm 99. An ASP typically deploys, host, and manger access to an application”) (0078)), comprising:

at an application service provider (i.e., *"The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application")* (0078)) site,

a communicating (fig. 2) processor for accessing at least one database (i.e., *"The application profiles 188 may be embodied as a memory mapped files rather than files stored on a storage device 16 such as a hard drive 16" (0132) and Examiner asserts that in the specification defines "the database 138, otherwise called a memory device" (0042), and Llewellyn et al. discloses application 479, application profiles and image (user interface) are stored in memory 14 (fig. 8, 14))* asset containing data representing a plurality of user interface images (i.e., *"A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and horizontal scaleability" (0077) or "many applications 86 make use of API calls which draw simple shapes to display, often, an application 86 will make many such API calls to render an image" (0089)*) associated with a corresponding plurality of organizations (Fig. 15 shows that image "Subscriber entry Point 500" associated with "client Module 80a" and "provider Entry Point 502" associated with "Client Module 80b" and *"The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization")* (0109) and (Figs. 14-15)), and a plurality of executable procedures associated with the corresponding plurality of user interface images (i.e., *"A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and horizontal scaleability" (0077)*), an executable procedure supporting a user of a particular organization of said plurality of organization (i.e., *"companies, organizations" (0009)*) in managing access of employees of the particular organization (i.e., *"The authorization module 198 may also query a central services module 240 or some other database in order to discover which applications a particular user or workstation 94 is allowed to access" (0109) and "allowing user to access data and functionality specific to their session with an application 86" (0092) or "An entry point 480a,b may have a user interface 482a,b through which a user may control the*

application and view output. Each user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176)) to an application ("allowing user to access data and functionality specific to their session with an application 86" (0092))) hosted by an application service provider (i.e., "The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application" (0078), and used by said plurality of organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)); and

at least one repository (i.e., "all the data associated with such an object to the application 86 for storage or for access by the application 86" (0091)) including data represent an application and associated application data (i.e., "with such an object to the application 86 " (0091)) specific to said particular organization (i.e., "configuration data associated with a particular user or organization" (0109) or fig. 15);

a command processor (i.e., "processor 12 for processing software commands"(0069) (Fig. 1)) employing the at least one database (i.e., "a data entry application on a workstation that accesses a database that is on a server" (0013)) for initiating execution of a particular executable procedure organization (i.e., "companies, organizations" (0009)) in response to a command initiated at a remote location associated with the particular organization (Fig. 15 shows that image "Subscriber entry Point 500" associated with "Workstation 94a" and "provider Entry Point 502" associated with "Workstation 94b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or

organization") (0109)) using a particular user interface image (i.e., "a subscriber entry point 500 may include a **display module 510** which may capture screen shots of a **subscriber's workstation 94a**" (0181 and fig. 15)) associated with the particular executable procedure and with the particular organization (i.e., "configuration data associated with a particular user or organization" (109)), the particular executable procedure supporting the user in managing and granting access of an employee (i.e., "An ASP typically deploys, hosts, and **manages access** to an application, such as an application 86, to multiple users from a **centrally managed facility**" (0078)) of the particular organization to an application, an authorization processor for authorizing access of the user to a particular user interface image (i.e., "display module 510 which may capture screen shots of a **subscriber's workstation 94a**" (0181) or "enable one remote user to see and control the screen of a second remote user")(0027) or "The authorization module 198 may perform other functions in order to control access to services provided by the server module 160" (0109)) without intervention by the application service provider (Based on specification defines "without intervention by the application service" as managing their accounts, without requiring intervention by or cooperation with another party" (0010) and Llewellyn et al. discloses "the entry point **management module 148** may allow a user to connect to a particular entry point of an application 86...allowing user to access data and **functionality specific to their session** with an application"(0092) and Examiner asserts that the client can access to particular entry point and **management their functionality and data** without intervention with another the client. For particular, example, Fig. 15 shows client 80a can access to 500 to manage their functionality and data without intervention by client 80b) and excluding access by employees of organizations other than said particular organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" (0109) and "The authorization module 198 may also query a central services module 240 or some other database in order to discover which **applications a particular user or workstation 94** is allowed to access" (0109) and "allowing user

Art Unit: 2162

to access data and functionality specific to their session with an application 86" (0092) or "An entry point 480a,b may have a user interface 482a,b through which a user may control the application and view output. Each user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176).

Regarding to claim 17, Llewellyn et al. discloses a system enabling individual organizations of a plurality of different organizations (i.e., "many enterprises (companies, organizations, foundations, and the like) may rely on a central server to provide access to the Internet for all users on a local area network or wide area network served by the enterprise server owned by that company" (0009)) to manage access of their own respective employees (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)) to at least one remotely located application (i.e., "an application 86") (0078)) hosted by an application service provider (i.e., The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application") (0078)), comprising:

at an application service provider (i.e., "The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application") (0078)) site,

at least one database (i.e., "The application profiles 188 may be embodied as a memory mapped files rather than files stored on a storage device 16 such as a hard drive 16" (0132) and Examiner asserts that in the specification defines "the database 138, otherwise called a memory device" (0042), and Llewellyn et al. discloses application 479, application profiles and image (user interface) are stored in memory 14 (fig. 8, 14)) asset containing data representing a plurality of user interface images (i.e., "A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized

*administration and horizontal scalability" (0077) or "many applications 86 make use of API calls which draw simple shapes to display, often, an application 86 will make many such **API calls to render an image**" (0089)*

associated with a corresponding plurality of organizations (Fig. 15 shows that image "Subscriber entry Point 500" associated with "client Module 80a" and "provider Entry Point 502" associated with "Client Module 80b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109) and (Figs. 14-15)), and a plurality of executable procedures associated with the corresponding plurality of user interface images (i.e., "**A server farm 99 may be thought of as a group of servers that are linked together as a single system image** to provide centralized administration and horizontal scalability" (0077)), an executable procedure supporting a user of a particular organization of said plurality of organization (i.e., "**companies, organizations**" (0009)) in managing access of employees of the particular organization (i.e., "**The authorization module 198 may also query a central services module 240 or some other database in order to discover which applications a particular user or workstation 94 is allowed to access**" (0109) and "**allowing user to access data and functionality specific to their session with an application 86**" (0092) or "**An entry point 480a,b may have a user interface 482a,b through which a user may control the application and view output. Each user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a**" (0176) to an application ("allowing user to access data and functionality specific to their session with an **application 86**" (0092)))) hosted by an application service provider (i.e., "**The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application**" (0078), and used by said plurality of organization (i.e., "**The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization**") (0109)); and

at least one repository (i.e., “all the data associated with such an object to the application 86 for storage or for access by the application 86” (0091)) including data represent an application and associated application data (i.e., “with such an object to the application 86 “(0091)) specific to said particular organization (i.e., “configuration data associated with a particular user or organization” (0109) or fig. 15);

an authorization processor for authorizing access (i.e., “**identification data** 268, associations 270, and **authorizations** 272” (0123)) of the user to particular user interface image (i.e., “**many applications 86** make use of API calls which draw simple **shapes** to display, often, an application 86 will make many such API calls to render an image” (0089) or “the methods 486a of a subscriber entry point 500 may include a display module 510 which may capture screen shots of a subscriber's workstation 94a. The provider entry point 502 may have a **viewing module 512** that displays the captured display the screen shots on the provider's workstation 94b. In this manner the provider may see whatever the subscriber is seeing on his/her computer screen” (0181) and Examiner asserts plurality of user interface (“the entry point 500”, “entry point 502”) can be viewed and associated with particular origination (workstation 94a, 94b)) and an associated particular executable procedure associated with the particular organization in response to received identification information of the user (i.e., “ **identification data** 268, associations 270, and **authorizations** 272” (0123)) and excluding organization access of the user and employees of the particular organization to user interface image and executable procedures and data associated with the organization (i.e., “The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization”) (0109) and “**identification data** 268, associations 270, and **authorizations** 272” (0123))

a command processor (i.e., “processor 12 for processing software commands”(0069) (Fig. 1)) employing the at least one database (i.e., “a data entry application on a workstation that accesses a

database that is on a server" (0013)) for initiating execution of a particular executable procedure organization (i.e., "companies, organizations" (0009)) in response to a command initiated at a remote location associated with the particular organization (Fig. 15 shows that image "Subscriber entry Point 500" associated with "Workstation 94a" and "provider Entry Point 502" associated with "Workstation 94b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" (0109)) using a particular user interface image (i.e., "a subscriber entry point 500 may include a display module 510 which may capture screen shots of a subscriber's workstation 94a" (0181 and fig. 15)) associated with the particular executable procedure and with the particular organization (i.e., "configuration data associated with a particular user or organization" (109)), the particular executable procedure supporting the user in managing and granting access of an employee (i.e., "An ASP typically deploys, hosts, and manages access to an application, such as an application 86, to multiple users from a centrally managed facility" 0078)) of the particular organization to an application, an authorization processor for authorizing access of the user to a particular user interface image (i.e., "display module 510 which may capture screen shots of a subscriber's workstation 94a" (0181) or "enable one remote user to see and control the screen of a second remote user" (0027) or "The authorization module 198 may perform other functions in order to control access to services provided by the server module 160" (0109)) without intervention by the application service provider (Based on specification defines "without intervention by the application service" as managing their accounts, without requiring intervention by or cooperation with another party" (0010) and Llewellyn et al. discloses "the entry point management module 148 may allow a user to connect to a particular entry point of an application 86...allowing user to access data and functionality specific to their session with an application" (0092) and Examiner asserts that the client can access to particular entry point and management their functionality and data without intervention with another the client. For particular, example, Fig. 15 shows client 80a can access to 500 to manage their functionality and data without

*intervention by client 80b) and excluding access by employees of organizations other than said particular organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" (0109) and "The authorization module 198 may also query a central services module 240 or some other database in order to discover which **applications a particular user or workstation 94 is allowed to access**" (0109) and "**allowing user** to access data and functionality specific to their session with an application 86" (0092) or "An entry point 480a,b may have a user interface 482a,b through which a user may control the application and view output. Each user interface 482a,b **may be different and allow access** to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have **a user interface 482a that allows a user to access data 484a and methods 486a**. Data 484a and methods 486a may be available exclusively to users **accessing the application through entry point 480a**" (0176).*

Regarding to claim 18, Llewellyn et al. discloses a system the authorization processor authorizes access of the user in response to a command initiated (i.e., "In entry point 480a,b may have a session initiation module 488a,b that allows users to connect to an application 479" (0177)) using the particular user interface image (Fig. 15 shows that image "Subscriber entry Point 500" associated with "Workstation 94a" and "provider Entry Point 502" associated with "Workstation 94b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109) and "the provider entry point 502 may have a viewing module 512 that **displays the captured display the screen shots** on the provider's workstation 94b" (0181)).

Regarding to claim 19, Llewellyn et al. discloses a system enabling individual organizations of a plurality of different organizations (i.e., "many enterprises (companies, organizations, foundations, and the like) may rely on a central server to provide access to the Internet for all users on a local area network or wide area network served by the enterprise server owned by that company" (0009)) to manage access of their own respective employees (i.e., "The server configuration module 196

may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)) to at least one remotely located application (i.e., "an application 86") (0078)) hosted by an application service provider (i.e., The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application") (0078)), comprising:

at an application service provider site and accessed via a firewall (i.e., "communicate through HTTP handshaking. This may help past fire walls and work with fire walls and server farms" (0203))

at an application service provider (i.e., "The server farm 99 may be an Application Service Provider ("ASP") farm 99. An ASP typically deploys, host, and manger access to an application") (0078)) site,

at least one database (i.e., "The application profiles 188 may be embodied as a memory mapped files rather than files stored on a storage device 16 such as a hard drive 16" (0132) and Examiner asserts that in the specification defines "the database 138, otherwise called a memory device" (0042), and Llewellyn et al. discloses application 479, application profiles and image (user interface) are stored in memory 14 (fig. 8, 14)) asset containing data representing a plurality of user interface images (i.e., "A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and horizontal scaleability" (0077) or "many applications 86 make use of API calls which draw simple shapes to display, often, an application 86 will make many such API calls to render an image" (0089))

associated with a corresponding plurality of organizations (Fig. 15 shows that image "Subscriber entry Point 500" associated with "client Module 80a" and "provider Entry Point 502" associated with "Client Module 80b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109) and (Figs. 14-15)), and a plurality of executable procedures associated with the corresponding plurality of user interface images (i.e., "A server farm 99 may be thought of as a group of servers that are linked together as a single system image to provide centralized administration and

*horizontal scalability" (0077)), an executable procedure supporting a user of a particular organization of said plurality of organization (i.e., "companies, organizations" (0009)) in managing access of employees of the particular organization (i.e., "The authorization module 198 may also query a central services module 240 or some other database in order to discover which **applications a particular user or workstation 94 is allowed to access**" (0109) and "**allowing user to access data and functionality specific to their session with an application 86**" (0092) or "An entry point 480a,b may have a user interface 482a,b through which a user may control the application and **view output**. Each user interface 482a,b **may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b**. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176)) to an application ("allowing user to access data and functionality specific to their session with an **application 86**" (0092))) hosted by an application service provider (i.e., "The server **farm 99** may be an Application Service Provider ("**ASP**") farm 99. An ASP typically deploys, host, and manger access to an application" (0078), and used by said plurality of organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)); and*

a command processor (i.e., "processor 12 for processing software commands"(0069) (Fig. 1)) employing the at least one database (i.e., "a data entry application on a workstation that accesses a database that is on a server" (0013)) for initiating execution of a particular executable procedure organization (i.e., "companies, organizations" (0009)) in response to a command initiated at a remote location associated with the particular organization (Fig. 15 shows that image "Subscriber entry Point 500" associated with "Workstation 94a" and "provider Entry Point 502" associated with "Workstation 94b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or

organization") (0109) and "In entry point 480a,b may have a session **initiation module 488a,b** that allows users to connect to an application 479" (0177)) using a particular user interface image (i.e., "a subscriber entry point 500 may include a **display module 510** which may capture screen shots of a **subscriber's workstation 94a**" (0181 and fig. 15)) associated with the particular executable procedure and with the particular organization (i.e., "configuration data associated with a particular user or organization" (109)), the particular executable procedure supporting the user in managing and granting access of an employee (i.e., "An ASP typically deploys, hosts, and **manages access** to an application, such as an application 86, to multiple users from a **centrally managed facility**" 0078)) of the particular organization to an application, an authorization processor for authorizing access of the user to a particular user interface image (i.e., "display module 510 which may capture **screen shots of a subscriber's workstation 94a**" (0181) or "enable one remote user to see and control the **screen** of a second remote user")(0027) or "The authorization module 198 may perform other functions in order to control access to services provided by the server module 160" (0109)) without intervention by the application service provider (Based on specification defines "without intervention by the application service" as managing their accounts, without requiring intervention by or cooperation with another party" (0010) and Llewellyn et al. discloses "the entry point **management module 148** may allow a user to connect to a particular entry point of an application 86...allowing user to access data and **functionality specific to their session** with an application"(0092) and Examiner asserts that the client can access to particular entry point and **management their functionality and data** without intervention with another the client. For particular, example, Fig. 15 shows client 80a can access to 500 to manage their functionality and data without intervention by client 80b) and excluding access by employees of organizations other than said particular organization (i.e., "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" (0109) and "The authorization module 198 may also query a central services module 240 or some other database in order to

Art Unit: 2162

discover which applications a particular user or workstation 94 is allowed to access" (0109) and "allowing user to access data and functionality specific to their session with an application 86" (0092) or "An entry point 480a,b may have a user interface 482a,b through which a user may control the application and view output. Each user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 4-6, and 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Llewellyn et al. (U.S. pub. No. 2003/0061279 A1) in view of Gavrilu et al. (U.S. Pub. No. 2002/0026592 A1).

With respect to claim 4, Llewellyn et al. discloses wherein the authorization processor excludes access to the user and employees of the particular organization to data associated with organization other than the particular organization (*i.e.*, "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization") (0109)) but Llewellyn et al. does not disclose removing permission of the user and employees of the particular organization to access the data associated with the other organizations from a directory of permissions used to control data access. However, Gavrilu et al. discloses wherein

removing permission of the user and employees of the particular organization to access the data associated with the other organizations (*i.e.*, “among users and roles of different organizations” (0010)) from a directory of permissions used to control data access (*i.e.*, “automatically **removing the role** from the access control lists of all abstract objects accessible to that role; automatically deleting the association between the role and all abstract **objects accessible to that role**; automatically recalculating permissions and granting permissions to the instance of each first encountered role instantiated on a host computer or set of host computers” (0032)) . It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Llewellyn et al.’s system by adding the function to remove the permission of the user and employees of the particular organization to access the data in order to have to associate object based upon a permitted accessibility thereby, minimizing redundant storage while maximizing security the system for the stated purpose has been well known in the art as evidenced by teaching of Gavrilla et al. (0018-0019).

With respect to claim 5, Gavrila et al. discloses wherein a Microsoft compatible Active Control List (ACL) (*i.e.*, “The preferred embodiment stores that permission using the usual mechanism of ACLs (Access Control Lists).” (0112)) (the motivation is the same as claim 4).

With respect to claim 6, Gavrila et al. discloses wherein the authorization processor removes the permission of the user and employees of the particular organization in responses to addition of the particular organization as a new organization to the plurality of organizations (*i.e.*, “Adding a new permission-inheritance arc to the directed acyclic graph, automatically **removing the role** from the access control lists of all abstract objects accessible to that role” (0032) and Examiner asserts that “responses to addition of particular” is equivalent with

automatically removing the role...when adding a new permission) (the motivation is the same as claim 4).

Regarding claim 8, Gavrilă et al. discloses wherein an executable procedure enables the user to **at least one of add** an employee and remove an employee, of an organization as a user entitled to access the application hosted by the application service provider (i.e. *"adding the member of the first role instance to the instance of the second role and to all instance of the roles that inherit the membership of the second role"* (0197) and Examiner asserts that *"adding the member of the first role to the instance the second role"* and therefore, the numbers (employees or users) of second role are added.) (The motivation is the same as claim 4).

Regarding claim 9, Gavrilă et al. discloses wherein the executable procedure changes authorization information associated with add or remove employee (i.e. *"adding the member of the first role instance to the instance of the second role and to all instance of the roles that inherit the membership of the second role"* (0197)) (the motivation is the same as claim 4).

(10) Response to Argument

I. (Issue): Rejection of claims 1-3, 7 and 10-19 under 35 U.S.C 102(e).

a. In the first argument, the Appellant state *"Llewellyn describes enabling remote access and control of applications located at multiple locations...it is respectfully submitted that the rejection of claims 2, 7, 10, 11 and 13-15 under 35 U.S.C. 102(b) be withdrawn"* as recited in claim 1 of the present arrangement." Pages 8-11.

Appellant alleges the defects found in the rejection under 35 U.S.C 102, holding claims 1-3, 7 and 9-10 anticipated by Llewellyn. Appellant contents that Llewellyn does not discloses or suggest a "particular executable procedure supporting the user in

Art Unit: 2162

managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization following login to said application and without intervention by the application service provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization".

Appellant's allegation has not been found persuasive. In a direct contradiction to appellant's content, Llewellyn all of the limitations of claim s1-3, 7 and 9-110. For clarity, the paragraphs supporting the limitations have been categorized in the box below.

Claim	Llewellyn	Explain
The particular executable procedure supporting the user in managing and granting access of an employee of the particular organization without intervention by the application service provider and	<i>"An ASP typically deploys, hosts, and manages access to an application, such as an application 86, to multiple users from a centrally managed facility" (0078), "display module 510 which may capture screen shots of a subscriber's workstation 94a " (0181) or "enable one remote user to see and control the screen of a second remote user" (0027) or "The authorization module 198 may perform other functions in order to control access to services provided by the server module 160" (0109), "the entry point management module 148 may allow a user to connect to a particular entry point of an application 86...allowing user to access data and functionality specific to their session with an application" (0092) and Examiner asserts that the client can access to particular entry point and management their functionality and data without intervention with another the client. For particular, example, Fig. 15 shows client 80a</i>	Examiner asserts that each application is associated with one of interface image (0089) or fig. 15. and Based on specification defines "without intervention by the application service" as managing their accounts, without requiring intervention by or cooperation with another party" (0010) and Examiner asserts that the client can access to particular entry point and management their functionality and data without intervention with another the client. For particular, example, Fig. 15 shows client 80a can access to 500 to manage their functionality and data without intervention by client 80b

Art Unit: 2162

	<i>can access to 500 to manage their functionality and data without intervention by client 80b)</i>	
excluding access to said application data specific to said particular organization by employees of of organizations other than said particular organization	<i>"The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" (0109) and "The authorization module 198 may also query a central services module 240 or some other database in order to discover which applications a particular user or workstation 94 is allowed to access" (0109) and "allowing user to access data and functionality specific to their session with an application 86" (0092) or "An entry point 480a,b may have a user interface 482a,b through which a user may control the application and view output. Each user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176).</i>	

Thus, Llewellyn discloses all the limitations of claimed invention such as "user of particular organization of said plurality of organization in managing access...without intervention by the application service provide" since the paragraph 0109 discloses "an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" and Examiner asserts that "administrator" is "user of particular organization". Further, Llewellyn discloses at paragraph 0118, an editing module 256 may permit editing by an appropriate **authorized individual** accessing the database record 250 or the principal engine

accessed by other interface modules in order to permit appropriate editing of databases records 250 in accordance with selected authorization (0118)(databases records 250 content the users profile, identifications and authorization of individual user of particular organization of plurality of organizations (fig. 6)). Examiner asserts that "authorized individual" (0118) of reference is the "user of particular organization of plurality of organizations in managing access " of claimed invention that can access to databases records 250 to edit the files to manage access of employees of particular organization or plurality of organization. Further more, Llewellyn discloses at abstract the "enabling multiple users to access and **control the same instance of a running application**" and Examiner asserts that "multiple users" are user of particular organization of said plurality of organizations.

Examiner cited paragraph [0092] (see on the rejection above or on categorized in the box above) to show the granting access of an employee of the particular organization to an application **without intervention** of the application server provider and excluding access to said application data specific to said particular organization by employees of organizations other than said particular organization". Examiner asserts that the user in managing and granting access of an employee of the particular organization of plurality of organizations in Llewellyn's system by using the databases records 250 and has been edited by "authorized individual", it means the user of particular organization of plurality organizations has authorized to edit the databases records 250 to grand permit to individual employee of particular organization (0118) to access.

In view of the above remarks, Llewellyn discloses all features claimed in the present claimed arrangement.

b. In the second argument, the Appellant state *"Dependent claim 3 dependent on claim 1 and is considered patentable for the reason presented above with respect to claim 1....Consequently, it is respectfully submitted that the rejection of claim 3 under 35 U.S.C 102 (b) be withdrawn."* pages 11-12.

Appellant contents that Llewellyn does not discloses or suggest a "the authorization processor excludes access of the user and employees of the particular organization to user interface images and executable procedures and data associated with organizations other than particular organization".

Appellant's allegation has not been found persuasive. In a direct contradiction to appellant's content, Llewellyn discloses the claimed authorization processor which "excludes access" (*"An entry point 480a, b may have a user interface 482a, b through which a user may control the application and view output. Each user interface 482a,b may be different and allow access to data 484a,b and methods 484a,b unique to a particular entry point 480a,b. For example entry point 480a may have a user interface 482a that allows a user to access data 484a and methods 486a. Data 484a and methods 486a may be available exclusively to users accessing the application through entry point 480a" (0176)*) to "user interface images and executable procedures and data associated with organization other than the particular organization" (*Fig. 14 shows "the interface 482a", "the interface 482b" images and data associated with organization other than the particular organization and Fig. 15 shows that image "Subscriber entry Point 500" associated with "Workstation 94a" and "provider Entry Point 502" associated with "Workstation 94b" and "The server configuration module 196 may also enable an administrator to set up accounts which may include authentication and configuration data associated with a particular user or organization" (0109) and "In entry*

*point 480a,b may have a session **initiation module** 488a,b that allows users to connect to an application 479"*

(0177)). Further, Examiner indicates on remark above, the "**administrator**" or "**authorized individual**" (0118) can be the user of particular organization or plurality organization. Therefore, Llewellyn discloses all limitations of claimed 3 invention.

c. In the third argument, the Appellant state "*Dependent claim 12 is dependent on independent claim 1 and is considered patentable for the reason presented above with respect to claim 1. Additionally, claim 12 is also considered patentable because the features claimed are not anticipated by Llewellyn...submitted that the rejection of claim 12 under 35 U.S.C. 102 (b) be withdrawn*" page 12.

Appellant contents that Llewellyn does not discloses or suggest a "prevent replication of user identification information between two employees of different organizations of the plurality of organizations".

Examiner does not agree with Applicant's argument since Applicant admitted that Llewellyn discloses identifying a user and authenticating user (page 12, line 27) and Llewellyn discloses the "authorized individual" can access to modify or editing the identification and authenticating user (paragraph 0118) and **prevent unauthorized** access to a server (0110). Therefore, user identification information is not been replication between two employees of different organizations of the plurality of organization.

d. In the fourth argument, the Appellant state "*independent claim 16 provides a system enabling an individual organization of a plurality of*

different...Consequently, it is respectfully requested that the rejection of claim 16 under 35 U.S.C. 102(e) be withdrawn" pages 13-16.

Appellant argues the same as first argument and Examiner's remarks above at response on first Appellant's argument.

e. In the fifth argument, the Appellant state *"Independent claim 17 provides a system enabling individual organizations of a plurality of different organizations to manage access of their own respective employees to at least one remotely located application hosted by an application...it is respectfully submitted that the rejection of claim 18 under 35 U.S.C. 102 (b) be withdrawn."* pages 16-20.

Appellant argues the same as first argument and Examiner's remarks above at response on first Appellant's argument.

f. In the sixth argument, the Appellant state *"Independent claim 19 provides a user interface system enabling individual organizations of a plurality of different organizations to ...Consequently, it is respectfully requested that the rejection of claim 19 under 35 U.S.C. 102 (e) be withdrawn."* pages 20-23.

Appellant argues the same as first argument and Examiner's remarks above at response on first Appellant's argument.

II. (Issue): Rejection of claims 4-6, 8 and 9 under 35 U.S.C. 103(a).

g. In the first argument, the Appellant state *"Claim 4 is dependent upon independent claim 1 and is allowable for reasons presented above with respect to claim 1. Specifically, Llewellyn does not disclose or suggest the claimed features of the present arrangement...Consequently, it is respectfully requested*

that the rejection of claims 4 and 5 under 35 U.S.C 103 (a) be withdrawn" pages 24-26.

Appellant alleges the defects found in the rejection under 35 U.S.C 103, holding claim 4 anticipated by Llewellyn and Gavril. Appellant contends that Llewellyn and Gavril does not disclose or suggest a "particular executable procedure supporting the user in managing and granting access of an employee of the particular organization to said application and said associated application data specific to said particular organization flowing login to said application and without intervention by the application service and excluding access to said application data specific to said particular organization by employees of organization other than said particular organization".

Appellant's allegation has not found persuasive. In a direct contradiction to appellant's content, Llewellyn discloses clear all the limitation recited above of claimed invention (see Examiner's remark on part a above). Further, Llewellyn discloses at paragraph 0118, an editing module 256 may permit editing by an appropriate **authorized individual** accessing the database record 250 or the principal engine **accessed by other interface modules** in order to permit appropriate editing of databases records 250 in accordance with selected authorization (0118)(databases records 250 content the users profile, identifications and authorization of individual user of particular organization of plurality of organizations (fig. 6)). Examiner asserts that "authorized individual" (0118) of reference is the "user of particular organization of plurality of organizations in managing access " of claimed invention that can access to databases records 250 to edit the files to manage access of employees of particular

organization or plurality of organization. Therefore, Llewellyn alone discloses editing the data records 250, that means can adding or removing permission of the user and employees of particular organization by editing by "authorized individual" of particular organization of plurality of organizations. Furthermore, Gavrila clearly discloses removing permission of the user and employees of the particular organization to access the data associated with the other organizations (see paragraph 0032). The claim recites "removing permission of the user and employees of the particular organization" and Gavrila discloses removing the role from the access control lists for particular user and employees of the particular organization from the control list. Therefore, combine Llewellyn and Gavrila discloses all limitations recited on claim 4.

Examiner does not agree with Appellant since combining the two system are operable device since both system are used to control access for particular user of organization of plurality of organizations. The combination the two systems would function since an administrator or authorized individual would edit the control access list (databases records 250 on Llewellyn's system) or set security permission for server or to granting access to a role in a RBAC system.

h. In the second argument, the Appellant state "*Dependent claim 6 is dependent on claims 1 and 4 and is considered patentable for the reasons presented above with respect ...the rejection of claim 6 under 35 U.S.C 103 (a) be withdrawn*" pages 26-27.

Examiner does not agree with Appellant since Llewellyn and Gavrila disclose all limitations recited on claim 4 (see Examiner's remark on part g above). Further, Gavrila

discloses wherein removes the permission of the user and employees of the particular organization in response to addition of the particular organization as a new organization to the plurality of organizations since Gavrilla discloses wherein automatic revocation and recalculation of permissions on object instances for role instances where roles are removed (paragraph 0027). Therefore, when addition or remove of the particular organization or object role, the Gavrilla's system will automatic revocation and recalculation of permissions as the same of claimed invention of claim 6.

- i. In the third argument, the Appellant state "*Dependent claim 8 is dependent on claim 1 and is considered patentable for the reasons presented above with respect to claims 1...Consequently, it is respect submitted that the rejection of claims 4-6, 8 and 9 under 35 U.S.C. 103 (a) be withdrawn.*" pages 27-28.

Examiner does not agree with Appellant since Llewellyn and Gavrill discloses all limitations of claimed invention (See Examiner's remarks on part h above). Further, Llewellyn discloses at paragraph 0118, an editing module 256 may permit editing by an appropriate **authorized individual** accessing the database record 250 or the principal engine **accessed by other interface modules** in order to permit appropriate editing of databases records 250 in accordance with selected authorization (0118)(databases records 250 content the users profile, identifications and authorization of individual user of particular organization of plurality of organizations (fig. 6)). Examiner asserts that "authorized individual" (0118) of reference is the "user of particular organization of plurality of organizations in managing access " of claimed invention that can access to

Art Unit: 2162

databases records 250 to edit the files to manage access of employees of particular organization or plurality of organization or adding or remove an employee of organization. Therefore, Llewellyn alone discloses editing the data records 250, that means can adding or removing the user and employees of particular organization by editing by "authorized individual" of particular organization of plurality of organizations. Further, Gavrilla discloses adding a member of a first role to instance of a second role is equivalent with adding the an employees. Therefore, combination of Llewellyn and Gavrila disclose all limitations of claimed invention.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Hung T Vy/

Primary Examiner, Art Unit 2163

Conferees:

Don Wong Spe Au 2163

/don wong/

Supervisory Patent Examiner, Art Unit 2163

/John Breene/

Supervisory Patent Examiner, Art Unit 2162

Art Unit: 2162

/Hung T Vy/

Primary Examiner, Art Unit 2163